

FIG. 1

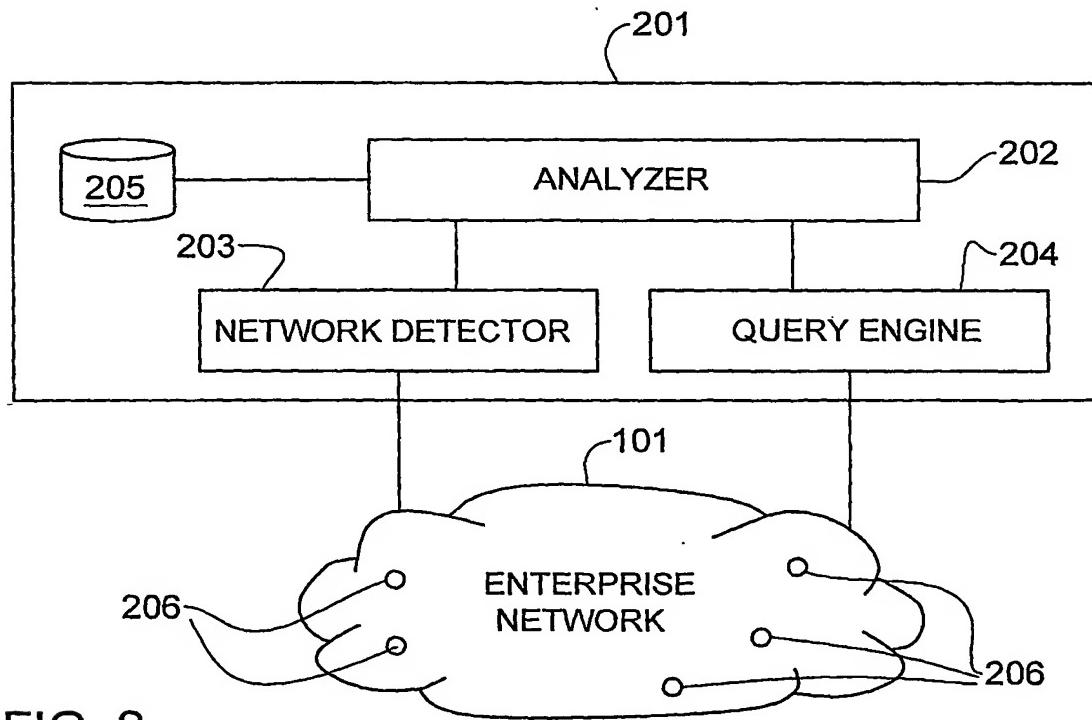


FIG. 2

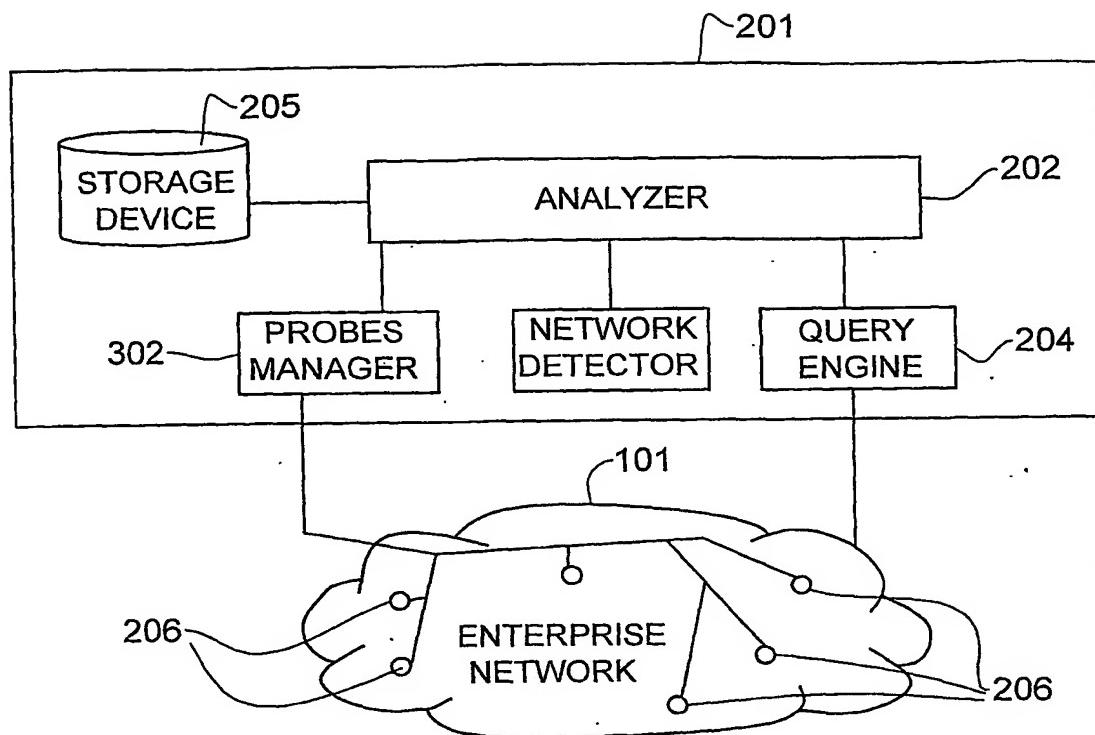


FIG. 3

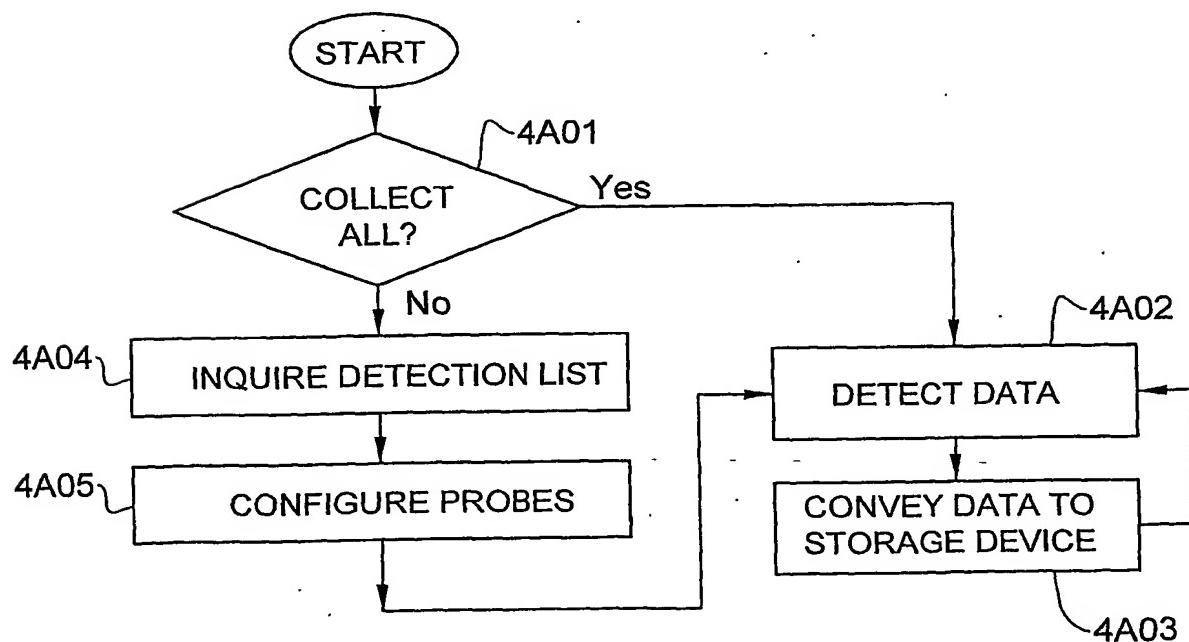


FIG. 4A

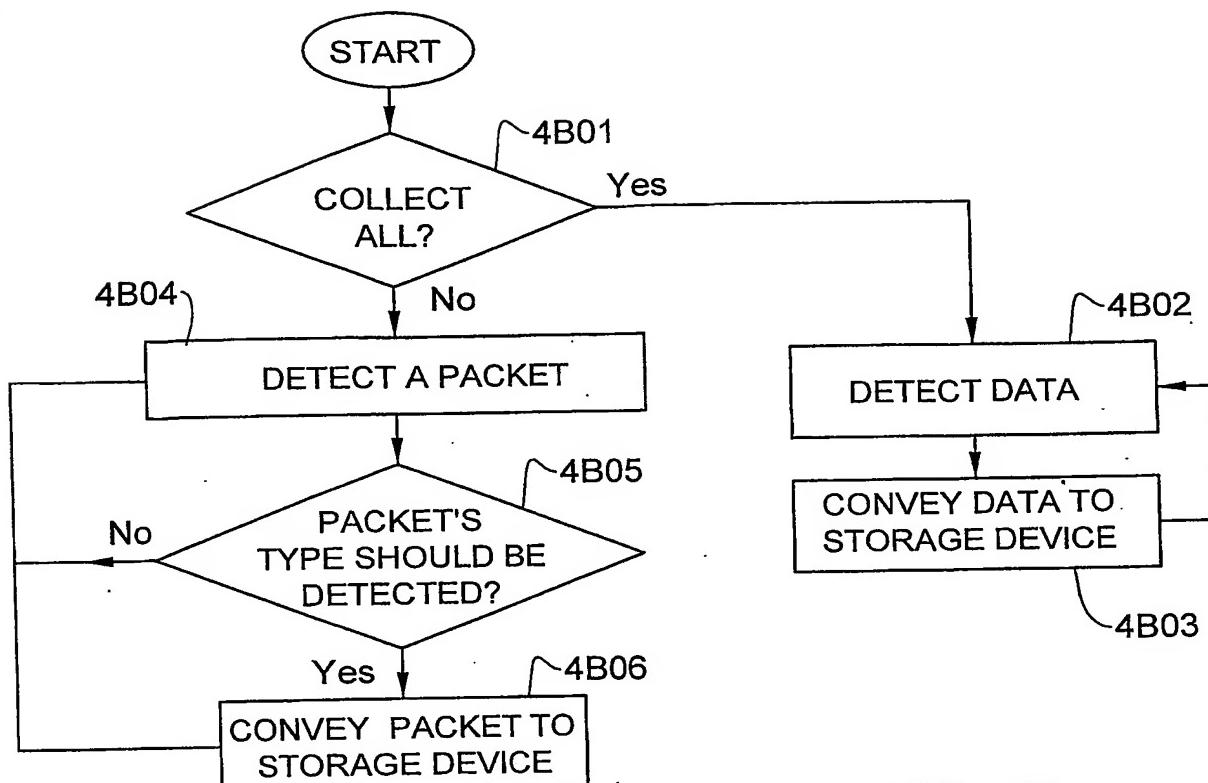


FIG. 4B

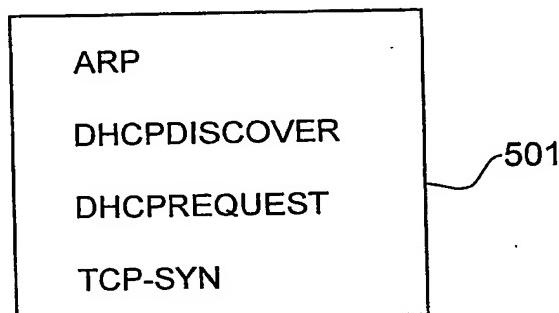


FIG. 5

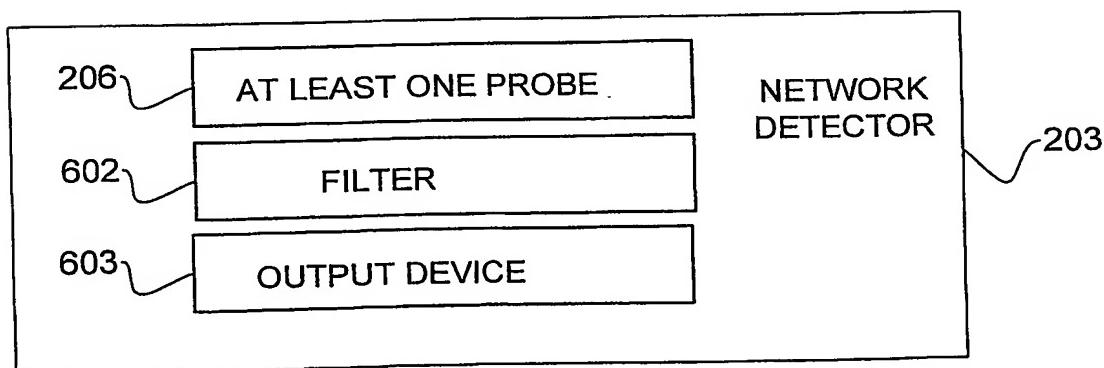


FIG. 6

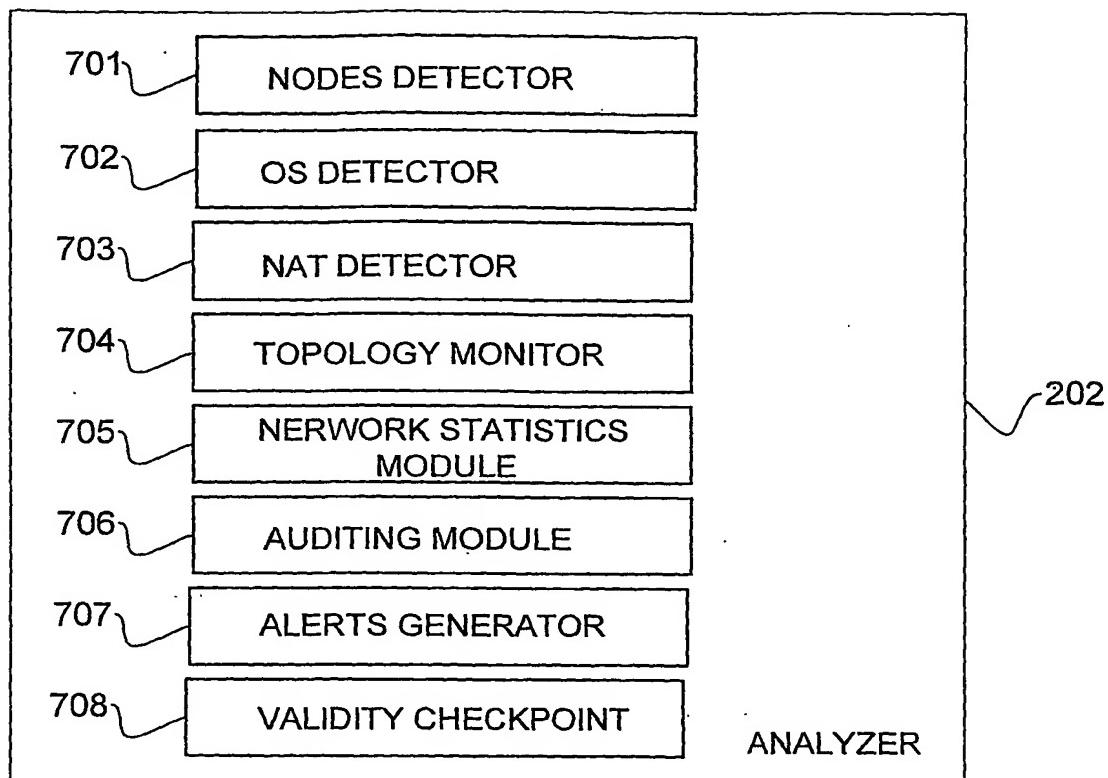


FIG. 7

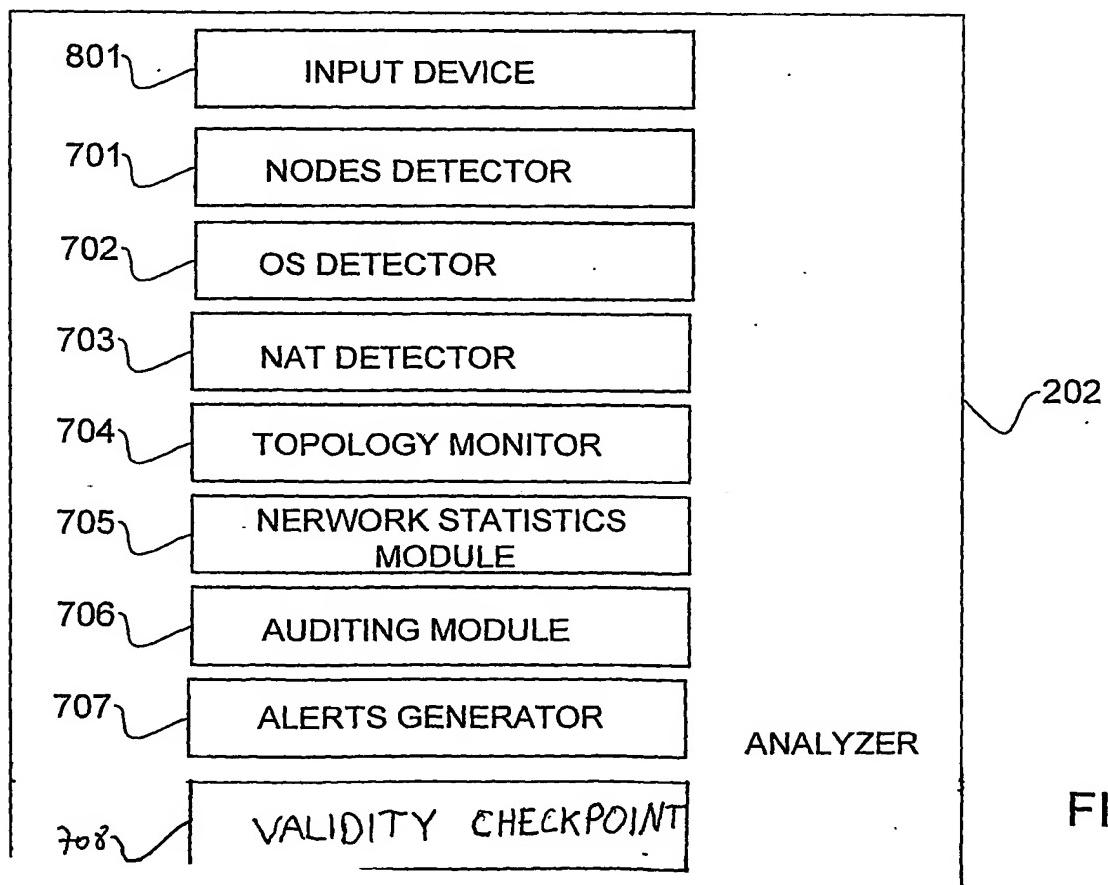


FIG. 8

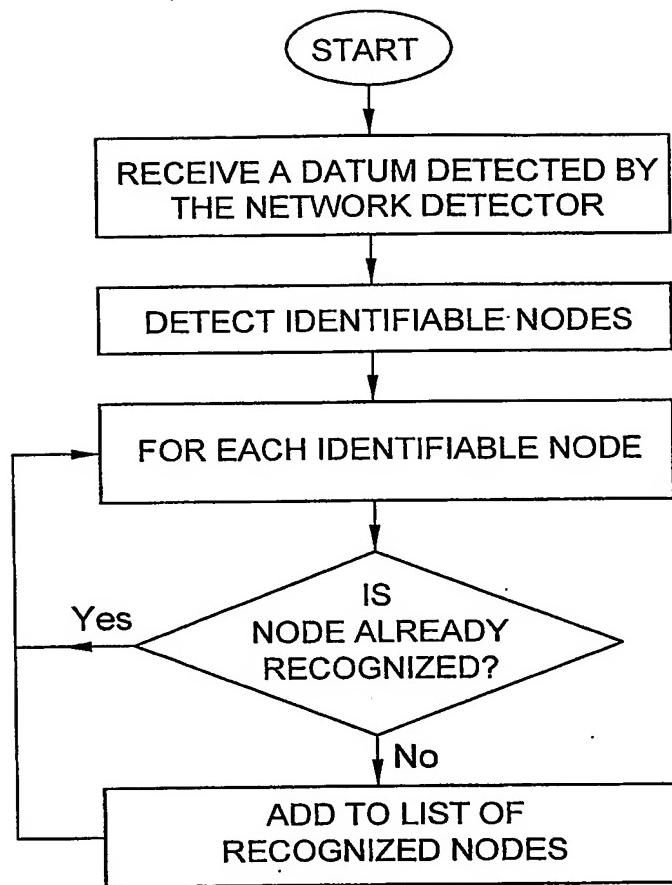


FIG. 9

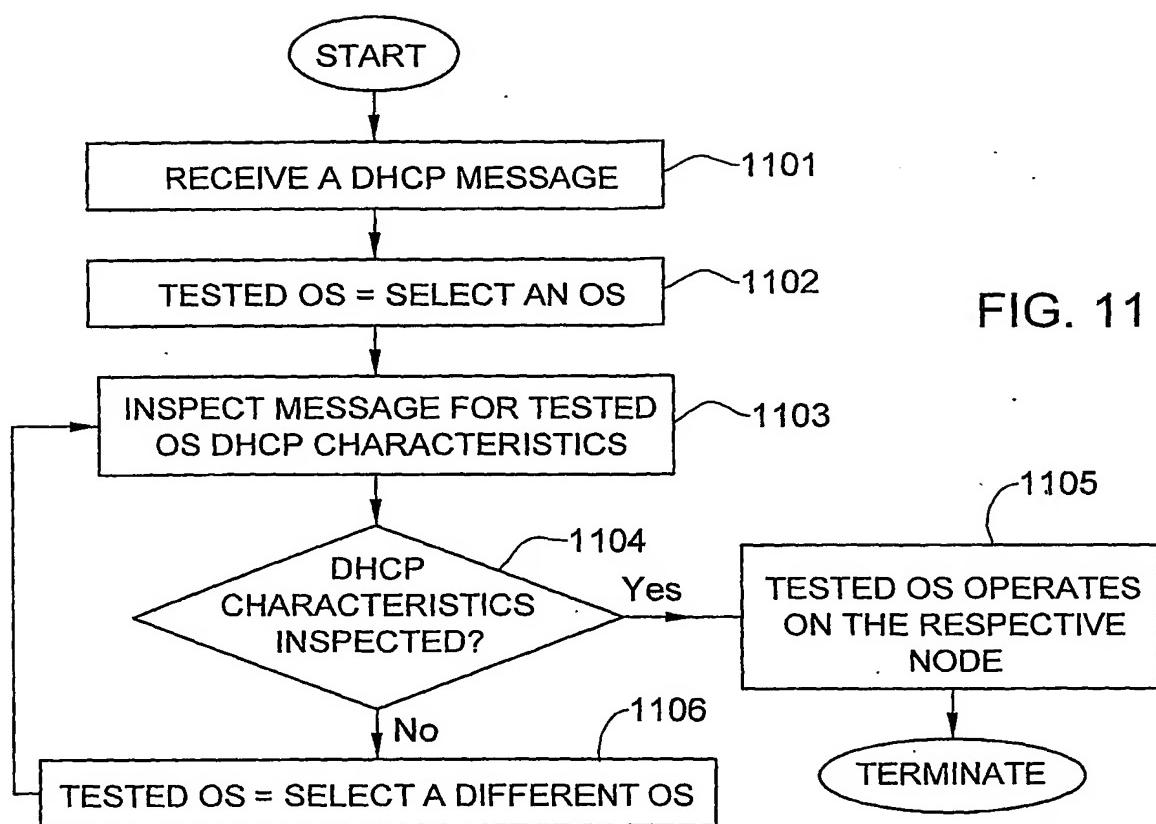
Option 53: DHCP Message Type
Option 116: DHCP Auto-Configuration
Option 61: Client Identifier
Option 50: Requested IP Address
Option 12: Host Name
Option 60: Vendor class identifier = "MSFT 5.0"
Option 55: Parameter Request
 1 - Subnet Mask
 15 - Domain Name
 3 - Router
 6 - Domain Name Server
 44 - NetBIOS over TCP/IP Name Server
 46 - NetBIOS over TCP/IP Node Type
 47 - NetBIOS over TCP/IP Scope
 31 - Perform Router Discovery
 33 - Static Router
 249 - (Unknown Option Code)
Option 43 - Vendor Specific Information

~1001

Option 53: DHCP Message Type
Option 251: (Unknown Option Code)
Option 61: Client Identifier
Option 50: Requested IP Address
Option 12: Host Name
Option 60: Vendor class identifier = "MSFT 5.0"
Option 55: Parameter Request
 1 - Subnet Mask
 15 - Domain Name
 3 - Router
 6 - Domain Name Server
 44 - NetBIOS over TCP/IP Name Server
 46 - NetBIOS over TCP/IP Node Type
 47 - NetBIOS over TCP/IP Scope
 31 - Perform Router Discovery
 33 - Static Router
Option 43 - Vendor Specific Information

~1002

FIG. 10



OS_ID = Linux Kernel 2.4.18
 tcp_syn_window_size = 5840
 tcp_syn_IP_ID = !0
 tcp_syn_DF = 1
 tcp_syn_TTL = 64
 tcp_syn_options_order =
 "mss (1460) sackok timestamp (!0,0) NOP wscale (0)"
 tcp_syn_size = 60

OS_ID = FreeBSD 5.0
 tcp_syn_window_size = 65535
 tcp_syn_IP_ID = !0
 tcp_syn_DF = 1
 tcp_syn_TTL = 64
 tcp_syn_options_order =
 "mss (1460) NOP wscale (1) NOP NOP timestamp (!0,0)"
 tcp_syn_size = 60

FIG. 12

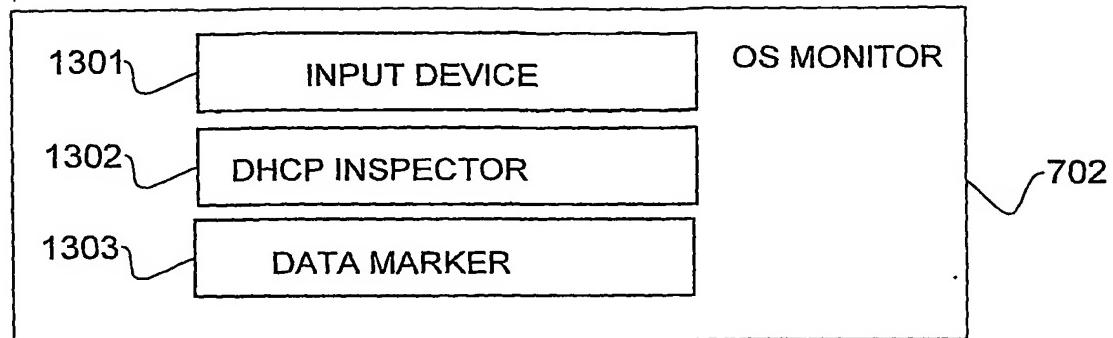


FIG. 13

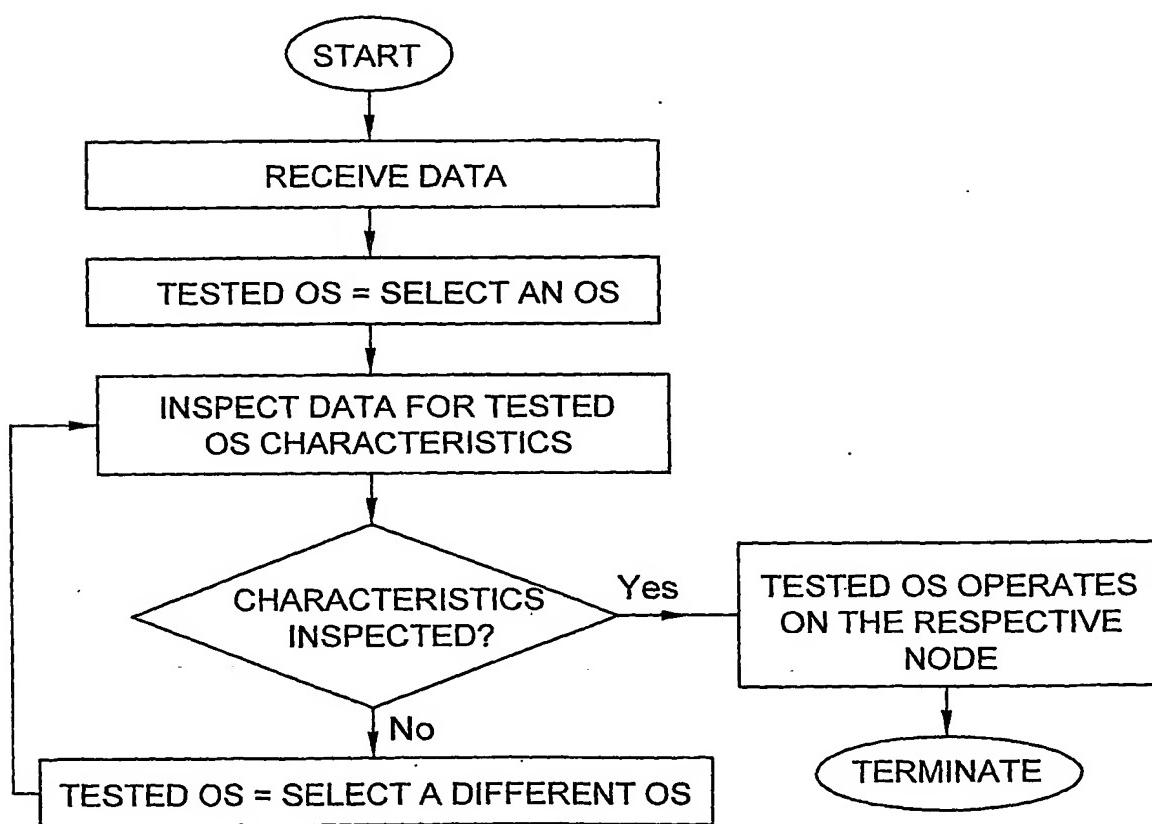


FIG. 14

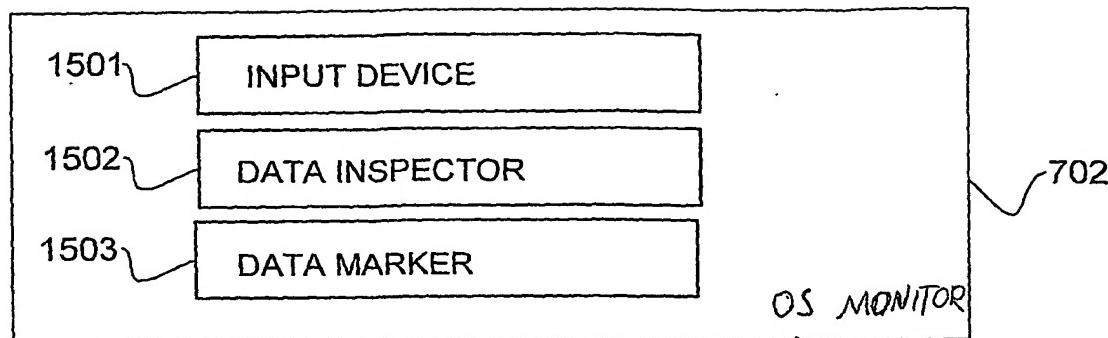


FIG. 15

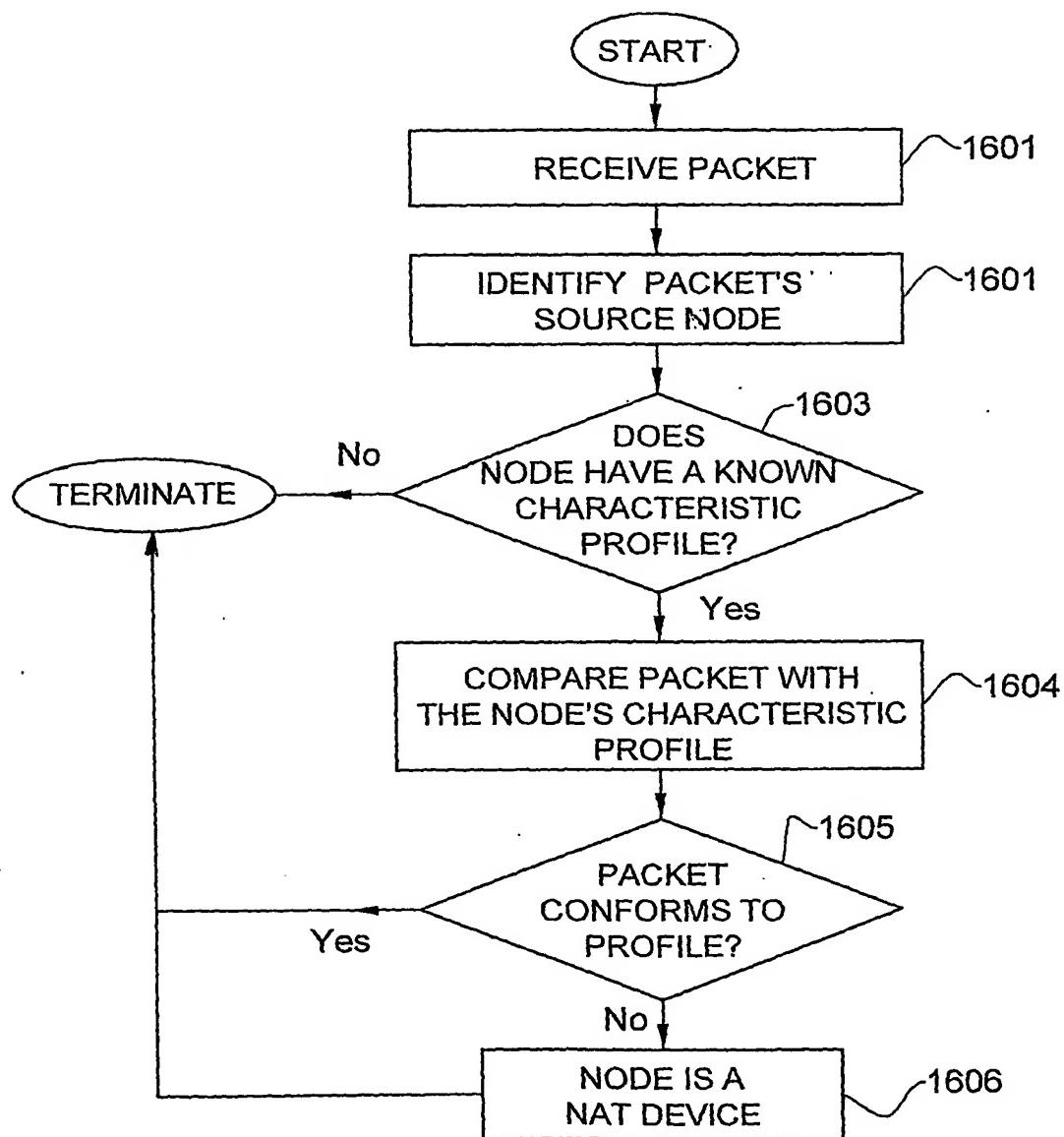


FIG. 16

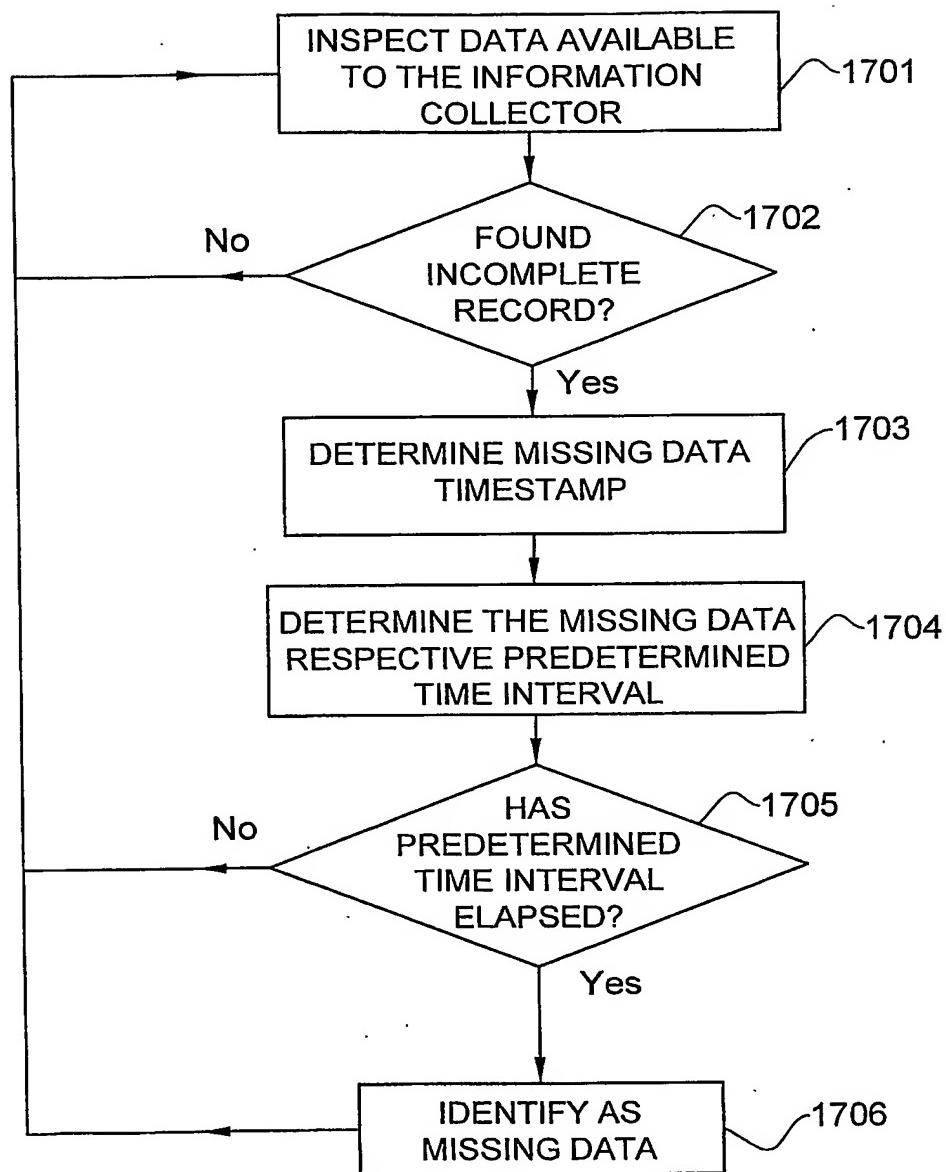


FIG. 17

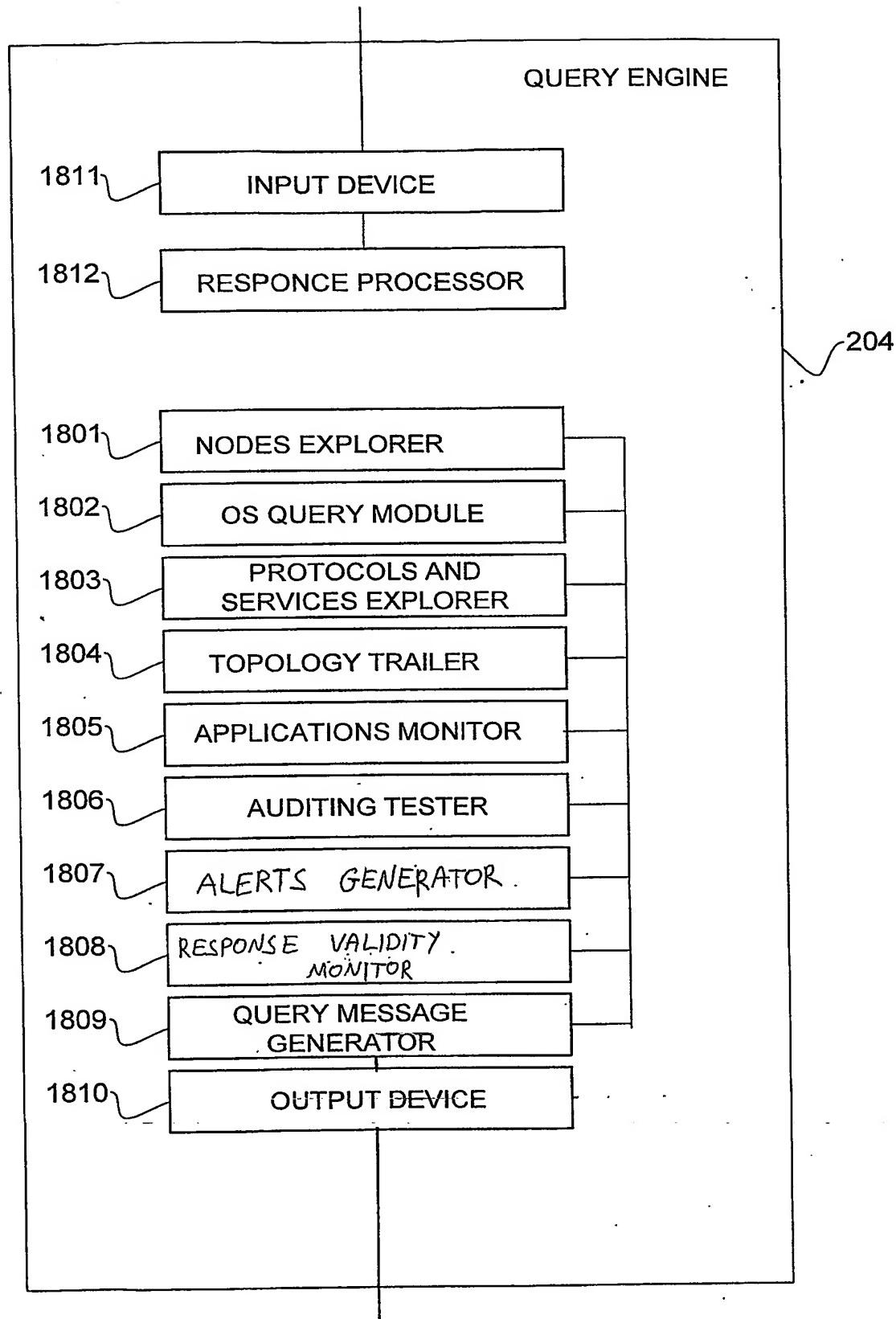


FIG. 18

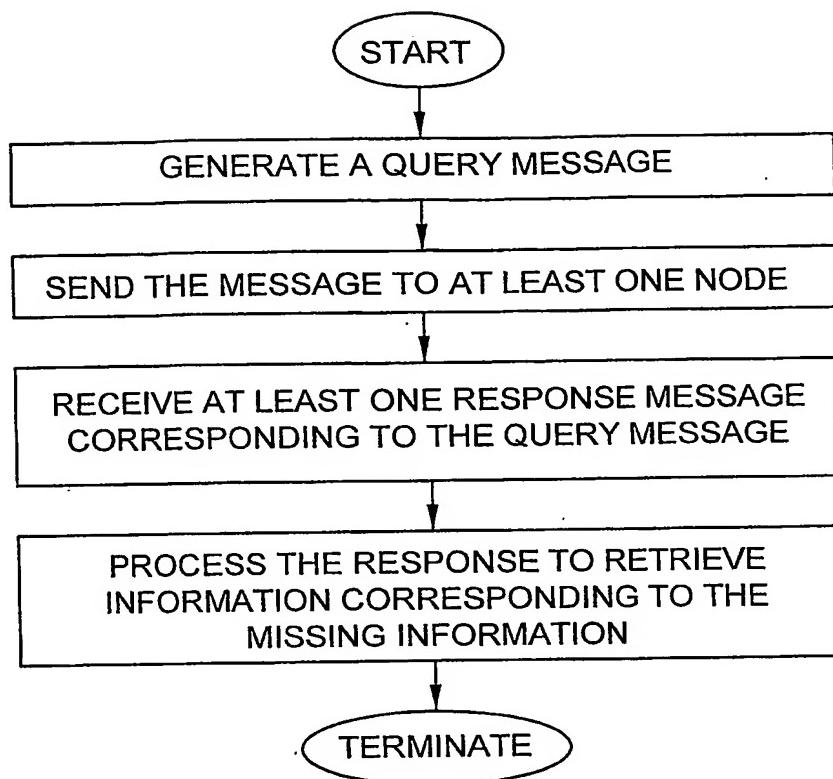


FIG. 19

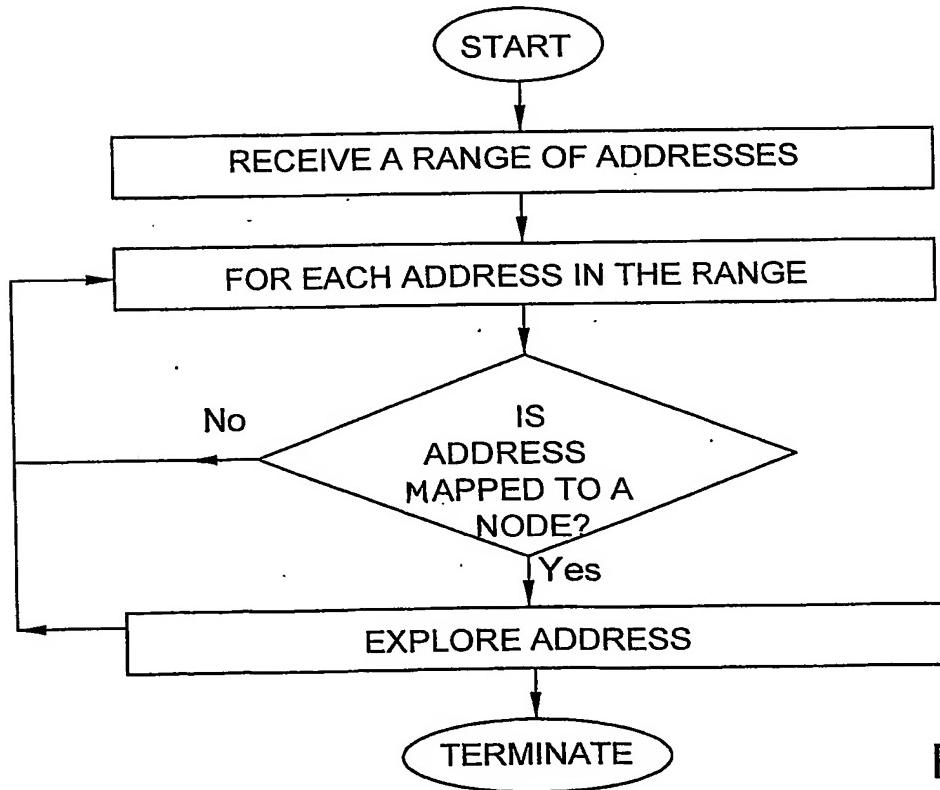


FIG. 20

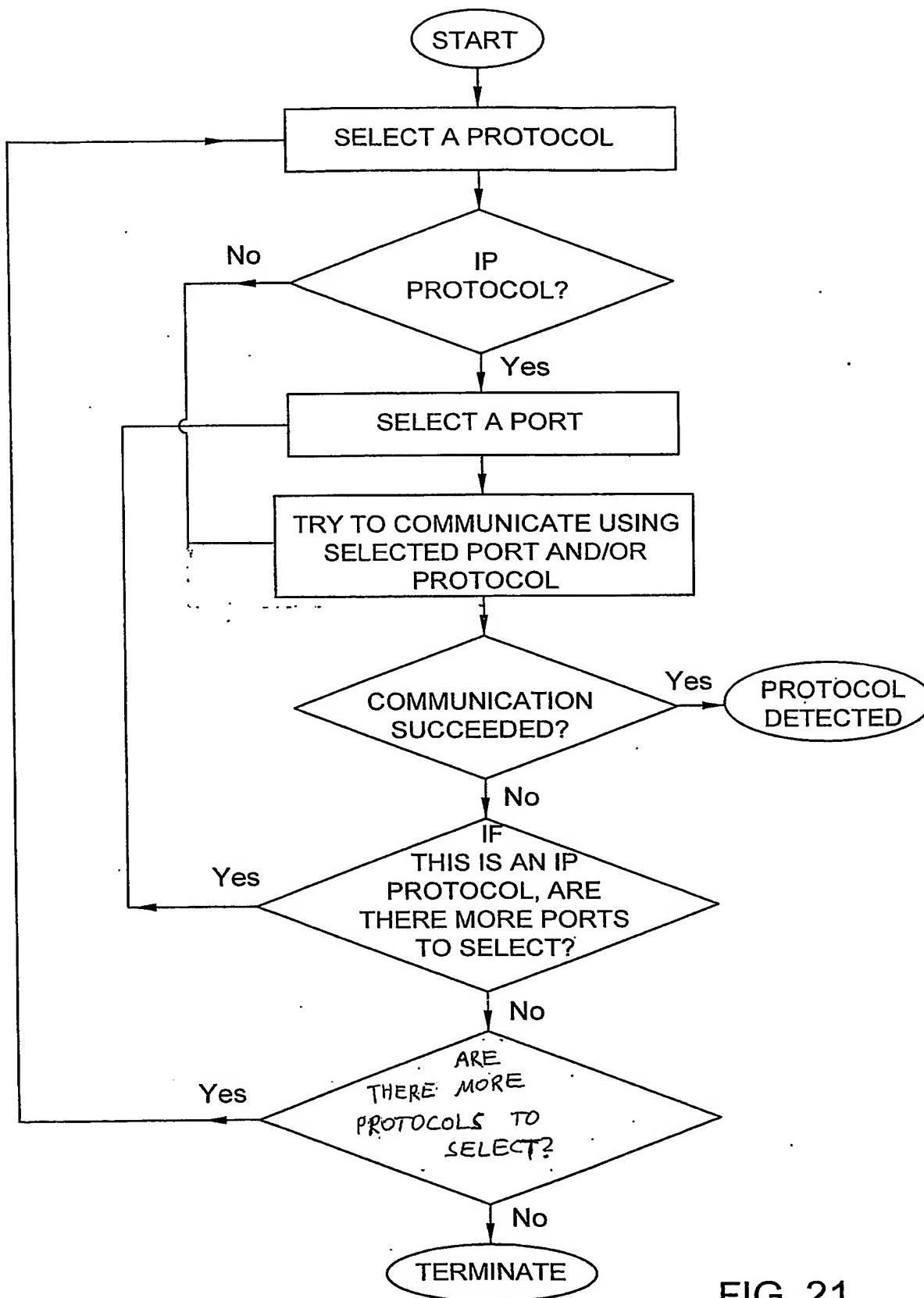


FIG. 21

Fig. 22A

```
fingerprint {

    OS_ID = "Microsoft Windows 2000"

    # Sub-Module A
    icmp_echo_code = 0
    icmp_echo_ip_id = !0
    icmp_echo_tos_bits = 0
    icmp_echo_df_bit = 1
    icmp_echo_reply_ttl = < 128

    # Sub-Module B
    icmp_timestamp_reply = y
    icmp_timestamp_reply_ttl = <128
    icmp_timestamp_reply_ip_id = !0

    # Sub-Module C
    icmp_addrmask_reply = n
    icmp_addrmask_reply_ttl = <128
    icmp_addrmask_reply_ip_id = !0

    # Sub-Module D
    icmp_info_reply = n
    icmp_info_reply_ttl = <128
    icmp_info_reply_ip_id = !0}
```

Fig. 22A (Cont.)

```
# Sub-Module E
#IP_Header_of_the_UDP_Port_Unreachable_error_message
    icmp_unreach_echoed_dtsize = 8
    icmp_unreach_reply_ttl = <128
    icmp_unreach_precedence_bits = 0
    icmp_unreach_df_bit = 0
    icmp_unreach_ip_id = !0

    #Original_data_echoed_with_the_UDP_Port_Unreachable_error_message
    icmp_unreach_echoed_udp_cksum = OK
    icmp_unreach_echoed_ip_cksum = OK
    icmp_unreach_echoed_ip_id = OK
    icmp_unreach_echoed_total_len = OK
    icmp_unreach_echoed_3bit_flags = OK

    # Sub-Module F [TCP SYN | ACK Module]
    #IP header of the TCP SYN | ACK
    tcp_syn_ack_tos = 0
    tcp_syn_ack_df = 1
    tcp_syn_ack_ip_id = !0
    tcp_syn_ack_ttl = <128

    #Information from the TCP header
    tcp_syn_ack_ack = 1
    tcp_syn_ack_window_size = 17520
    tcp_syn_ack_options_order = "MSS NOP WSCALE NOP
    NOP TIMESTAMP NOP NOP SACK"
    tcp_syn_ack_wscale = 0
    tcp_syn_ack_tsval = 0
    tcp_syn_ack_tsecr = 0
}
```

Fig. 22B

```
fingerprint {

    OS_ID = "Microsoft Windows 2003 Server "

    # Sub-Module A
    icmp_echo_code = 0
    icmp_echo_ip_id = !0
    icmp_echo_tos_bits = 0
    icmp_echo_df_bit = 1
    icmp_echo_reply_ttl = < 128

    # Sub-Module B
    icmp_timestamp_reply = y
    icmp_timestamp_reply_ttl = <128
    icmp_timestamp_reply_ip_id = !0

    # Sub-Module C
    icmp_addrmask_reply = n
    icmp_addrmask_reply_ttl = <128
    icmp_addrmask_reply_ip_id = !0

    # Sub-Module D
    icmp_info_reply = n
    icmp_info_reply_ttl = <128
    icmp_info_reply_ip_id = !0}
```

Fig. 22B (Cont.)

```
# Sub-Module E
#IP_Header_of_the_UDP_Port_Unreachable_error_message
    icmp_unreach_echoed_dtsize = >64
    icmp_unreach_reply_ttl = <128
    icmp_unreach_precedence_bits = 0
    icmp_unreach_df_bit = 0
    icmp_unreach_ip_id = !0

    #Original_data_echoed_with_the_UDP_Port_Unreachable_error_message
    icmp_unreach_echoed_udp_cksum = OK
    icmp_unreach_echoed_ip_cksum = OK
    icmp_unreach_echoed_ip_id = OK
    icmp_unreach_echoed_total_len = OK
    icmp_unreach_echoed_3bit_flags = OK

    # Sub-Module F [TCP SYN | ACK Module]
    #IP header of the TCP SYN | ACK
    tcp_syn_ack_tos = 0
    tcp_syn_ack_df = 1
    tcp_syn_ack_ip_id = !0
    tcp_syn_ack_ttl = <128

    #Information from the TCP header
    tcp_syn_ack_ack = 1
    tcp_syn_ack_window_size = 17520
    tcp_syn_ack_options_order = "MSS NOP WSCALE NOP
    NOP TIMESTAMP NOP NOP SACK"
    tcp_syn_ack_wscale = 0
    tcp_syn_ack_tsval = 0
    tcp_syn_ack_tsecr = 0
}
```